REMARKS

In the Office Action, the Examiner rejected claims 1, 3-6, 9-11, 13-19, 22-27, and 29-35. By this paper, claims 36-40 have been added. As such, claims 1, 3, 6, 9-11, 13-19, 22-27, and 29-40 are pending. In view of the following remarks, Applicants respectfully request reconsideration and allowance of all pending claims.

Response to Amendment

In the Office Action, the Examiner stated:

> The Applicant has incorrectly reinstated previously cancelled claims 2, 21, and 28. 37 C.F.R. 1.121(c)(5) states that a previously cancelled claim may be reinstated **only** by adding the claim as a "new" claim with a new claim number. See also 37 C.F.R. 1.126. For purposes of examination, the Examiner has renumbered claims 2, 21, and 28 as 33, 34, and 35 respectively.

Office Action, page 2 (emphasis in original). Applicants would like to thank the Examiner for considering the referenced claims even though they were reinstated incorrectly. By this Response, Applicants have correctly labeled the referenced claims as the Examiner suggested above. Hence, claims 33-35 have been designated as "previously presented."

Rejections Under 35 U.S.C. § 101

In the Office Action, the Examiner rejected claims 1, 3-6, 9-11, and 33 under 35 U.S.C. § 101 "because the claimed invention is directed to non-statutory subject matter because it includes no tangible result." Office Action, page 2. Applicants respectfully traverse this rejection.

Legal Precedent

According to the Supreme Court, congress intended statutory subject matter to "include anything under the sun that is made by man." *Diamond v. Chakrabarty*, 447 U.S. 303, 308-09; 206 U.S.P.Q. 193, 197 (1980). Indeed, exclusions of statutory subject matter are limited to laws of nature, natural phenomena and abstract ideas. *See Diamond v. Diehr*, 450 U.S. 175, 185; 209 U.S.P.Q. 1, 7 (1981). Other than these specific exceptions, therefore, nearly anything man made is statutorily patentable subject matter under 35 U.S.C. §101.

In determining when process or method claims include statutory subject matter, the Supreme Court in *Diehr* stated that "[t]ransformation and reduction of an article 'to a different state or thing' is the clue to the patentability of a process claim that does not include particular machines." *See id.* 450 U.S. at 183-185, 209 U.S.P.Q. at 6. In addition to the Supreme Court's transformation and reduction test, the Federal Circuit has developed a second test which may also be used to determine if a claim recites statutory subject matter, namely does the claim produce a "useful, concrete, and tangible result." *In re Alappat*, 31 U.S.P.Q.2d 1545, 1557 (Fed. Cir. 1994) (*en banc*). The Federal Circuit further elaborated on this second test by holding that one must look to "the essential characteristics of the subject matter, in particular, its practical utility." *State Street Bank & Trust Co. v. Signature Financial Group Inc.*, 47 U.S.P.Q.2d 1596, 1602 (Fed. Cir. 1998).

However, explaining this "useful, concrete, and tangible" test, the Federal Circuit has stated "the dispositive inquiry is whether the claim *as a whole* is directed to statutory subject matter." *In re Alappat*, 31 U.S.P.Q.2d at 1557. Indeed, there has been no requirement from

Congress, the Supreme Court, or the Federal Circuit mandating that a *specific final result* be shown for a claim to qualify under Section 101. *See id.* Rather, the Federal Circuit has specifically stated "the *Alappat* inquiry simply requires an examination of the contested claims to see if the claimed subject matter *as a whole* is a disembodied mathematical concept representing nothing more than a 'law of nature' or an 'abstract idea,' or if the mathematical concept has been reduced to *some practical application rendering it 'useful'*." *AT&T Corp. v. Excel Communications, Inc.*, 50 U.S.P.Q.2d 1447, 1451 (Fed. Cir. 1999) (emphasis added). Therefore, if a claim meets either the transformation and reduction test put forth by the Supreme Court, or if the claim, read as a whole and in light of the specification, produces any useful, concrete, and tangible result, the claim meets the statutory requirements of Section 101. *See id.*

Applicants respectfully assert that the independent claims 1, 13, 19 and 27, taken as a whole, each recite statutory subject matter under 35 U.S.C. §101 because they produce a useful, concrete and tangible result. The present Application is directed to generating a strong random number for use in a cryptographic security system. *See* Abstract. Specifically, the present application discloses methods and apparatuses for initializing and restoring security data which is used to generate keys for the cryptographic security algorithm. *See* Specification, p. 13, lines 18-22; p. 23, lines 4-15. The result of the initialization or restoration of security data is a fully populated or randomized seed pool, which may be indicated by a state bit, or alteration of a signature value stored in the seed pool. *See id.* at p. 17, lines 7-22; p. 24 line 6 to p. 25, line10.

Accordingly, independent claim 1 recites, *inter alia*, "A method of generating a random number for a cryptographic security subsystem of a processor-based device, the method comprising the acts of...writing one or more bits of data to a seed pool...and examining the state bit to determine whether the seed pool is full." Independent claim 13 recites, *inter alia*, "A method of initializing a seed pool for generating a random number for a cryptographic security subsystem of a processor-based device, the method comprising the acts of...writing one or more bits of data to the seed pool...enabling the cryptographic subsystem when more than a predetermined portion of the signature value of the seed pool has been altered." Independent claim 19 recites, *inter alia*, "A processor-based device comprising...a communications management system...wherein the communications management system comprises...security logic...wherein the security logic is configured to...examine the state bit to determine whether the seed pool is fully populated; write one or more bits of data to the seed pool." Independent claim 27 recites, *inter alia*, "A processor-based device comprising...a communications management system...wherein the communications management system comprises...security logic...wherein the security logic is configured to... write one or more bits of data to the seed pool, the bits altering a signature value; determine whether the plurality of data bits in the seed pool has at least a portion of the signature value."

Each claim, therefore, taken as a whole, recites either a method or apparatus for creating a full or fully populated seed pool by writing bits to the seed pool. Applicants assert that the fully populated seed pool is a useful, concrete and tangible result. For example, the seed pool may be used for the generation of keys in a security system, as decribed in detail in the present Application. *See* Specification, p. 4, line 20 to p. 5, line 2; p.13, lines 18-22.

Accordingly, Applicants respectfully request withdrawal of the rejection of independent claims 1, 13, 19, and 27, as well as all claims dependent thereon, under 35 U.S.C. §101.

Rejections Under 35 U.S.C. § 103(a)

In the Office Action, the Examiner rejected claims 1, 3-6, 9-11, 13-19, 22-27, and 29-35 under 35 U.S.C. § 103(a) as being unpatentable over Bruce Schneier's "Applied Cryptography", (hereinafter referred to as "the Schneier reference") and further in view of Utz et al., (U.S. Patent No. 5,680,131, hereinafter referred to as the "Utz reference"). Applicants respectfully traverse this rejection.

Legal Precedent

The burden of establishing a *prima facie* case of obviousness falls on the Examiner. *Ex parte Wolters and Kuypers*, 214 U.S.P.Q. 735 (PTO Bd. App. 1979). To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 180 U.S.P.Q. 580 (CCPA 1974). The mere fact that references *can* be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 16 U.S.P.Q.2d. 1430 (Fed. Cir. 1990). Accordingly, to establish a *prima facie* case, the Examiner must not only show that the combination includes *all* of the claimed elements, but also a convincing line of reason as to why one of ordinary skill in the art would have found the claimed invention to have been obvious in light of the teachings of the references. *Ex parte Clapp*, 227 U.S.P.Q. 972 (B.P.A.I. 1985).

Independent claims 1 and 19

Claim 1 recites, *inter alia*, "writing one or more bits of data to a seed pool upon termination of the first type of triggering event, the seed pool comprising a *state bit* indicative of a state of the seed pool... masking one or more bits of data to the seed pool upon termination of the second type of triggering event... examining the state bit to *determine whether the seed pool if full*." (Emphasis added). Claim 19 recites, *inter alia*, "a non-volatile memory device to store a seed pool, wherein the seed pool comprises a *state bit* indicative of the state of the seed pool...security logic...wherein the security logic is configured to...examine the state bit to *determine whether the seed pool if fully populated*...and mask one or more bits of data to the seed pool upon termination of the second type of triggering event." (Emphasis added).

In rejecting claims 1 and 19, the Examiner stated:

> Schneier fails to *specifically* mention determining if a seed pool is full or masking bits into the seed pool.
>
> Utz discloses the act of masking (serially combining) the one or more bits of data into the seed pool (UTZ col. 6 lines 57-61; col. 5 line 22) as well as determining if the seed pool is full; and writing one or more bits of data to the seed pool upon termination of the second type of triggering event if the seed pool is not full (UTZ col. 3 lines 38-40; col. 11 lines 51-55).

Office Action, p. 5. Applicants agree that the Schneier reference fails to disclose determining if a seed pool is full and masking bits into the seed pool. However, contrary to the Examiner's assertion, Applicants assert that the Utz reference fails to obviate the deficiencies of the Schneier reference. Specifically, the Utz reference fails to disclose examining a state bit to determine whether the seed pool is full.

The Utz reference is directed to a transmitting unit of a wireless security system. *See Utz,* col. 3, line 19. A pseudo-random number generator is used to generate a randomized synchronization code which is transmitted to a receiving unit. *See id.* at col. 3, lines 20-22. Verification codes are then generated by incrementing the pseudo-random number generator. *See id.*, col. 3, lines 22-40. The Utz reference also discusses some variable features of the transmitting unit, including the possibility of generating different synchronization codes after successive applications of power. *See id.* at col. 11, lines 50-55. However, the Utz reference *never* mentions examining a state bit to determine whether a seed pool is full. Indeed, the Utz reference does not even disclose a state bit.

As such, for at least this reason, the Utz reference fails to obviate the deficiencies of the Schneier reference with regards to independent claims 1 and 19. Accordingly, the Schneier reference and the Utz reference taken alone or in hypothetical combination, cannot support a *prima facie* case of obviousness under 35 U.S.C. §103 and Applicants respectfully request withdrawal of the rejection of independent claims 1 and 19.

Independent claims 13 and 27

In rejecting claims 13 and 27, the Examiner only refers to the Utz reference. The Utz reference, however, as has been pointed out in previous correspondence, fails to disclose all the elements of claims 13 and 27.

Claim 13 recites, *inter alia*, "A method of initializing a seed pool...comprising the acts of: (a) prior to enabling the cryptographic security subsystem, writing a plurality of bits

of data to a seed pool, the plurality of bits having a signature value...(c) writing one or more bits to the seed pool upon termination of the first type of triggering event, the one or more bits of data *altering the signature value of the seed pool*; and enabling the cryptographic security subsystem when more than a predetermined portion of the signature value of the seed pool has been altered." (Emphasis added). Claim 27 recites, *inter alia*, "A processor-based device comprising...a non-volatile memory device to store a seed pool comprising a plurality of data bits; and security logic in communication with ... the non-volatile memory device....wherein the security logic is configured to: write the one or more bits to the seed pool, the bits *altering a signature value*; determine whether a plurality of data bits in the seed pool has at least a portion of the signature value; and disable establishment of the secure communication session if the plurality of data bits has at least a portion of the signature value." (Emphasis added).

In contrast, the Utz reference does not disclose altering a signature value as set forth in claims 13 and 27. In rejecting claims 13 and 27, the Examiner correlated the "start value" of the Utz reference with the "signature value" of the present claims. *See* Office Action, p. 6. The "start value" of the Utz reference however, is never altered because it is used as an identifying value for a receiver to recognize a remote transmitting device. *See* Utz, col. 6, line 65 to col. 7 line 18. The "start value" is programmed to be specific to the particular transmitting unit, but several bits may be common to multiple transmitting units. *See id.* at col. 6, lines 30-35. To preclude alteration of the "start value," a disable fuse makes the nonvolatile memory where the "start value" is stored one-time programmable; thus, the start value is *fixed*. *See id.* col 8, line 58 to col. 9, line 4.

The "start values" are used in the generation of a "synchronization code." The transmitting unit of the Utz reference has an 11 bit RS/PRNG, a 13 bit RS/PRNG and a 16 bit RS/PRNG. *See* Utz, col 6, lines 37-61. The 11 bit RS/PRNG and 13 bit RS/PRNG are loaded with a "start value" from a non-volatile memory. *See id.* at col. 5, lines 34-42. When a pushbutton is depressed, the "start values" from the 11 bit RS/PRNG and the 13 bit RS/PRNG are serially supplied to a transmitter circuit. *See id.* at col. 6, lines 37-61. Additionally, the 16 bit RS/PRNG generates a pseudo random number which is serially supplied to the transmitting circuit. *See id.* The transmitting circuit then transmits a serial bit stream which includes the "start values" from the 11 and 13 bit RS/PRNG and the pseudo random number from the 16 bit RS/PRNG. *See id.* The serially-combined bit stream is called the "synchronization code." *See id.* Throughout this process, however, the "start values" are never altered. Indeed, as mentioned above, they are intended to remain *unaltered* so they can be used as an identifier for the transmitting unit.

As such, the Utz reference does not disclose altering a signature value as set forth in claim 13 and 27. For reasons similar to those set forth above with regards to claims 1 and 19, the Schneier reference fails to obviate the deficiencies of the Utz reference. Accordingly, the Utz reference and the Schneier reference, taken alone or in hypothetical combination, fail to disclose all the elements of claims 13 and 27. As such, a *prima facie* case for obviousness under 35 U.S.C. §103 has not been presented. Therefore, Applicants respectfully request withdrawal of the rejection of claims 13 and 27.

In view of the foregoing discussion, Applicants respectfully request withdrawal of the 35 U.S.C. §103 rejection and further request allowance of independent claims 1, 13, 19 and 27, as well as the allowance of all claims depending therefrom.

Conclusion

Applicants respectfully submit that all pending claims should be in condition for allowance. However, if the Examiner wishes to resolve any other issues by way of a telephone conference, the Examiner is kindly invited to contact the undersigned attorney at the telephone number indicated below.

Respectfully submitted,

Date: September 11, 2006

Michael G. Fletcher
Reg. No. 32,777
(281) 970-4545

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400